IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

TAWAINNA ANDERSON, Individually and as Administratrix of the ESTATE OF NYLAH ANDERSON, a deceased minor ***Plaintiff,*** **v.** **TIKTOK, INC. AND BYTEDANCE, INC.** ***Defendants***.	**No. 2:22-cv-01849-PD**

PLAINTIFF'S SUR-REPLY IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Robert J. Mongeluzzi
Jeffrey P. Goodman
Samuel B. Dordick
Rayna McCarthy
SALTZ MONGELUZZI & BENDESKY, P.C.
One Liberty Place
1650 Market Street, 52nd Floor
Philadelphia, Pennsylvania 19103
Tel.: (215) 496-8282
rmongeluzzi@smbb.com
jgoodman@smbb.com
sdordick@smbb.com
rmccarthy@smbb.com

Mark A. DiCello
DICELLO LEVITT GUTZLER LLC
Western Reserve Law Building
7556 Mentor Avenue
Mentor, Ohio 44060
Tel.: (440) 953-8888
madicello@dicellolevitt.com

Dated: August 18, 2022

Defendants' Reply continues to assert the same demonstrably incorrect arguments that were raised in their Motion concerning specific personal jurisdiction, immunity under the Communications Decency Act ("CDA"), and Pennsylvania products liability law. Defendants' arguments are unpersuasive, and the facts remain unchanged.

Defendants have purposefully availed themselves of Pennsylvania and either outright ignore or misrepresent their intentional collection of data directly from Nylah Anderson in Pennsylvania that ultimately gives rise to Plaintiff's claims. Instead of squarely addressing their intentional and directed data harvesting, Defendants confusingly argue that their purposeful actions in this regard are somehow unilateral actions taken by 10-year-old Nylah. Not true.

Defendants' CDA immunity arguments are similarly unavailing and ignore the fundamental reason why Plaintiff's claims do not seek to treat Defendants as publishers or speakers. The fact that Defendants could have satisfied their duties *without altering the content generated by third-parties*, strips them of any arguable CDA protection. *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1092 (9th Cir. 2021); *A.M. v. Omegle.com, LLC*, No. 3:21-cv-01674, 2022 WL 2713721, *4 (D. Or. July 13, 2022) (plaintiff's claims did not seek to treat defendant as a publisher or speaker because defendant "would not have to alter the content posted by its users—it would only have to change its design and warnings."). Defendants neglected to address

this critical issue and instead continued their efforts to shoehorn this case into the CDA by focusing on factual information within plaintiff's complaint which is immaterial to the maintenance of Plaintiff's claims. The CDA does not bar Plaintiff's claims.

Finally, Defendants ask this Court to ignore the fundamental policy considerations underlying Pennsylvania strict products liability law. These considerations command that the law adapt and evolve with technological advancements just as other courts have done in order to classify computer programs and software as "products." Defendants also urge this Court to disregard their own representations in pleadings in other actions which classify their app and algorithm as "products." The Court should do neither. Defendants' app and algorithm are products, and their defective and dangerous designs and lack of warnings that caused Nylah Anderson's death properly subjects Defendants to Pennsylvania strict products liability law.

I. Specific Personal Jurisdiction Exists.

Defendants glaringly avoid a direct discussion of their purposeful Pennsylvania-based data harvesting that gave rise to Plaintiff's claims. This is because it is fatal to their jurisdiction argument. As Plaintiff pointed out in her Opposition, Defendants intentionally reached into Pennsylvania and extracted data directly from Nylah's phone, other social media accounts, internet network, and

from Nylah's person (such as her biometric data) which was then utilized by Defendants' algorithm to target her. *See* D.E. 17 ("Opp.") at 5 (citing Defendants' Privacy Policy). This is unquestionably purposeful availment and Defendants' arguments to the contrary are meritless.

Defendants first argue that there cannot possibly be specific personal jurisdiction over them because the Blackout Challenge videos are available on their app all over the world. *See* D.E. 21 ("Reply") at 2. Defendants double down on this argument by claiming that the Privacy Policy is "widely applicable" and permits Defendants to extract users' data all over the world. *Id.* at 3. Defendants' argument essentially boils down to: "we purposefully avail ourselves *everywhere*, so you can't sue us *anywhere*." Defendants have not cited any authority which suggests that if a defendant is able to intentionally conduct business activities and purposefully avail itself in enough jurisdictions, specific jurisdiction cannot exist in any of them. No such authority exists and the law holds the exact opposite. *See Ford Motor Co. v. Montana Eighth Judicial District Court*, 141 S.Ct. 1017, 1027 (2021).

In an unsupported attempt to avoid the consequences of its intentional Pennsylvania-based conduct, Defendants preposterously claim that its collection of Pennsylvania-based data was Nylah's own doing. *See* Reply at 3 ("[t]o the extent there was 'Pennsylvania data,' its locus was admittedly controlled by Nylah and not purposefully targeted by Defendants."). Defendants' attempts to shift blame for

their own data collection efforts to Nylah is unsupported and defies logic. Further, Defendants could have easily decided not to extract massive amounts of data from Pennsylvania citizens, including Nylah Anderson, and jurisdiction may have been avoided. Defendants consciously chose not to, and they thus had clear notice they were subject to suit in Pennsylvania. *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119, 1126-27 (W.D. Pa. 1997). Notably, amongst the data they extracted, harvested and utilized was Nylah's location.

Defendants also argue that Plaintiff's allegations that their algorithm used the harvested data to target Nylah is contradicted by the fact that Blackout Challenge videos were seen "in other states and other countries[.]" Reply at 3. This is nonsensical and does nothing to chip away at the clear basis for holding specific personal jurisdiction over Defendants in this action. Just because Defendants' defective and dangerous algorithm may have also shown other vulnerable children choking videos in other states in no way means Nylah was not specifically targeted here. Indeed, this is the very reason why Plaintiff alleges the algorithm and app are defectively designed.

Specific personal jurisdiction over Defendants exists, and Defendants' motion should be denied.

II. Plaintiff's Claims Are Not Barred by the CDA.

Defendants' Reply repeatedly focuses on factual information in Plaintiff's Complaint pointing out that Defendants failed to timely remove Blackout Challenge videos or failed to prevent them from being posted in the first place. *See* Reply at 5-6. These factual allegations are immaterial to Plaintiff's core legal theory and allegations—Defendants' app and algorithm are defectively designed products that knowingly delivered a dangerous video to a vulnerable 10-year-old girl. As Plaintiff stated in her Opposition, "the Blackout Challenge can exist on TikTok without necessarily exposing TikTok to liability." Opp. at 17. Should the Court feel so inclined it may strike any such factual allegations (which are true but merely *dicta* in Plaintiff's Complaint) concerning Defendants' failure to remove the Blackout Challenge video or prevent it from being posted in the first place, but this does not result in the dismissal of Plaintiff's case. Plaintiff's case is, and always has been, about how Defendants' defectively designed product functioned to send the dangerous video directly to Nylah.

In focusing on immaterial aspects of Plaintiff's allegations, Defendants glaringly ignore the fundamental holding of *Lemmon*: the plaintiffs' claims did not seek to treat the defendant as a publisher or speaker because defendant "could have satisfied" its duty "to design a product more useful than it was foreseeably dangerous—***without altering the content that [defendant's] users generate***." 995

F.3d at 1092 (emphasis added). The focus of the *Lemmon* court's analysis was whether defendant could satisfy its alleged duty without altering user content and if defendant could, then CDA immunity did not apply. *Id.* Defendants aim to distract this Court from engaging in this determinative analysis because the outcome of such an analysis is inevitably a finding that Defendants could have satisfied their duty to design a non-defective product without altering any aspect of third-party content whatsoever. Defendants need not alter the Blackout Challenge video, their product just shouldn't knowingly send it to a 10-year-old.

Defendants emphasize footnote 4 of the *Lemmon* decision, which states that the plaintiffs could not fault the defendant for publishing third-party content generally on its app. *Id.* at 1093 n. 4. This *dicta* does nothing to support Defendants' arguments. Plaintiff here is not seeking to fault Defendants for simply publishing Blackout Challenge videos on its platform—indeed Plaintiff has unequivocally stated that the Blackout Challenge videos can exist on Defendants' platform without necessarily subjecting them to liability. Opp. at 17. Instead, Defendants' liability here is grounded in its defectively designed product taking deliberate action to target 10-year-old Nylah Anderson and send her the dangerous video. This is clearly distinguishable from the scenario discussed by the *Lemmon* court in footnote 4. The court stated, "allow[ing] its users to transmit user-generated content to one another does not detract from the fact that [a plaintiff] seek[s] to hold [the defendant] liable

for its role in violating its distinct duty to design a reasonably safe product." *Lemmon*, 995 F.3d at 1092.

The recent decision of *A.M. v. Omegle.com, LLC* confirms that this Court's determinative focus should be on whether Defendants can satisfy their alleged duties *without altering third-party content* (they can). 2022 WL 2713721, at *4. In *Omegle*, a 11-year-old user of an online chat room, called Omegle, was paired with a man in his late thirties who forced her to send him pornographic images and videos of herself. *Id.* at *1. After the man was apprehended by his local authorities, the minor brought a product liability action against Omegle alleging that the online chat room was defectively designed because it paired vulnerable minors, such as plaintiff, with adults. *Id.* at *1. Relying on *Lemmon*, ***the Omegle court held that the plaintiff's product liability claims were not subject to the CDA's immunity provisions*** because "Omegle could have satisfied its obligation to Plaintiff by designing its product differently" and because the plaintiff was "not claiming that Omegle needed to review, edit, or withdraw any third-party content to meet this obligation." *Id.* at *3. Omegle could have satisfied its obligations by simply not pairing an 11-year-old user with this adult for chatting purposes. This is analogous to how Defendants here could have satisfied their obligations by not sending a 10-year-old user a dangerous video.

The *Omegle* court also shot down the defendant's argument that its holding that the plaintiff's product liability claims were not subject to the CDA would contradict *Doe v. Twitter, Inc.*, 555 F.Supp.3d 889 (N.D. Cal. 2021). As noted by the *Omegle* court, the *Twitter* court found that the publication function, and thus the CDA, was implicated because, "[i]n other words…***Twitter would have to alter the content posted by its users***" by preventing the posting of third-party content containing child pornography. *Omegle*, 2022 WL 2713721, at *4 (quoting *Twitter*, 555 F.Supp.3d at 930) (emphasis added). Defendants' *Twitter* argument here fails for exactly the same reason (i.e. Defendants here would not need to edit content to satisfy their obligation to Plaintiff).

Defendants' reliance on *Gonzalez v. Google LLC*, 2 F.4th 871, 894 (9th Cir. 2021) serves them no better and *Gonzalez* only further emphasizes that Plaintiff's claims here are not subject to the CDA. In *Gonzalez*, the plaintiffs were family members of victims of fatal shootings in Paris, Istanbul, and San Bernardino, California which were committed by persons associated with designated terrorist groups. *Id.* 880-83. The plaintiffs brought claims under the Anti-Terrorism Act ("ATA"). *Id.* at 880. At bottom, the *Gonzalez* plaintiff's claims were founded on allegations that the defendants (Google, Twitter, and Facebook) shouldn't have allowed ISIS to post certain content on defendants' social media platforms. *Id.* at 880. The duty alleged by the *Gonzalez* plaintiffs was a simple "duty not to support

terrorists." *Id.* at 891. In order to satisfy the alleged duty, the defendants would have had to perform quintessential publisher functions such as deciding whether to alter third-party content, and the claims thus fell under the CDA.

Importantly, the *Gonzalez* plaintiff argued that the defendants' use of algorithms transformed them into information content *creators* that are explicitly exempt from immunity by the terms of the CDA. *Id.* at 892. This was the context of the *Gonzalez* court's algorithm discussion that Defendants emphasize, but it has nothing to do with Plaintiff's claims here. Plaintiff has never alleged that Defendants' use of algorithms transforms them into information content creators. Instead, Plaintiff alleges Defendants violated a distinct product liability duty to design a non-defective product and duties under common law negligence—claims and duties which were not discussed at all in *Gonzalez*. *Gonzalez* provides no guidance here.

In their Reply and Motion, Defendants repeatedly attempt to draw parallels between this case and those involving ones in which the plaintiffs sought to hold interactive computer service providers accountable under the ATA for terrorists using defendants' platforms to communicate. This is clearly not the case here. The more appropriate analogy is a situation in which a defendant's defectively designed algorithms detected an individual with extremist and anti-American views and intentionally fed that individual with content concerning the creation of homemade

bombs. It is hard to imagine a court condoning such behavior or finding that the defendant would be immunized under the CDA.

This Court's focus should properly be on the fundamental question of whether Defendants can satisfy their alleged duty—here, to design a non-defective product—without altering any third-party content. *Lemmon*, 995 F.3d at 1092; *Omegle*, 2022 WL 2713721, *4. It is apparent that Defendants could satisfy their duties without altering the third-party content whatsoever, and the CDA is thus inapplicable. Defendants' motion should be denied.

III. Defendants' App and Algorithm Are Products.

Defendants ask this Court to hold that computer software and programs, like Defendants' app and algorithm, are not "products" subject to Pennsylvania's product liability law. In doing so, Defendants regurgitate the same exact cases they cited in their Motion. Defendants' product is nothing like the professional design service at issue in *Snyder v. ISC Alloys, Ltd.*, 772 F.supp. 244 (W.D. Pa. 1991), and the other cases are distinguishable for the reasons discussed in Plaintiff's Opposition. Opp. at 22-24. Defendants offer nothing new at all aside from after-the-fact excuses for why Defendants represented their app and algorithm to be "products" in one court (*see* Opp. at 21) but "not products" in this Court. Defendants cannot recharacterize their product simply because it is convenient here. Defendants' app and algorithm are products, as other courts have found. *See* Opp. at 21-22 (collecting cases); *see also*

Omegle, 2022 WL 2713721, at *4 (treating the defendant's online chat room as a product that was subject to the plaintiff's product liability design defect claims).

Defendants also continue to urge this Court to draw the very "[b]right lines and broad rules" that "elevate the lull of simplicity over the balancing of interests embodied by the principles underpinning [the jurisprudence of the relevant area of law]" that the Pennsylvania Supreme Court has admonished. *Tincher v. Omega Flex, Inc.*, 103 A.3d 328, 425 (Pa. 2014). Pennsylvania product liability law must adapt along with technological innovations, and a finding that software and computer programs are not "products" will have disastrous consequences in a world that is becoming increasingly software based. Defendants have also not offered any proof that software and computer programs are "intangible" like the "ideas" and "expressions" at issue in the cases Defendants rely upon. To the contrary, computer software and programs *are* tangible. *See, e.g. Application of Bernhart*, 417 F.2d 1395, 1400 (Cust. & Pat. App. 1969) (United States Court of Customs and Patent Appeals stating that "if a machine is programmed in a certain new and unobvious way, ***it is physically different from the machine without that program***.") (emphasis added).

Defendants would argue that if a Tesla vehicle's autopilot software was programmed such that it functioned to steer the vehicle into oncoming traffic, the operators of the Tesla or the vehicles struck by the Tesla cannot bring a product

liability claim under Pennsylvania law because it was the defective software that caused the accident, and software is not a "product." Adopting Defendants' position and drawing such a "[b]right line[] and broad rule[]" that computer programs and software are not "products" will inevitably lead to absurd results.

Moreover, even if this Court were to agree with Defendants, contrary to Pennsylvania law, that Defendants' app and algorithm are not "products," this still should not result in the dismissal of Plaintiff's case. Plaintiff also pled a common law negligence claim. *See* D.E. 1 at Count II. Had a TikTok employee, in an effort to carry out his official job responsibilities, spied on 10-year-old Nylah and then used that information to determine Nylah was likely to view and partake in dangerous challenges involving choking activity, and texted the Blackout Challenge video to Nyah and said, "try this," there is little doubt that TikTok could be found negligent. This is what Plaintiff pled, and Defendants accomplishing this through an app does not change the calculus. Plaintiff also pled a claim for negligent failure to warn. *Id*. at ¶ 127(pp), (qq). This was the precise claim that survived dismissal efforts in *Doe v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016), and it should similarly survive here.

For all of the foregoing reasons, Defendants' Motion to Dismiss should be denied.

Dated: August 18, 2022

/s/ Robert J. Mongeluzzi
Robert J. Mongeluzzi
Jeffrey P. Goodman
Samuel B. Dordick
Rayna McCarthy
SALTZ MONGELUZZI & BENDESKY P.C.
One Liberty Place
1650 Market Street, 52nd Floor
Philadelphia, Pennsylvania 19103
Tel: (215) 496-8282
rmongeluzzi@smbb.com
jgoodman@smbb.com
sdordick@smbb.com
rmccarthy@smbb.com

Mark A. DiCello
DiCELLO LEVITT GUTZLER LLC
7556 Mentor Avenue
Western Reserve
Law Building
Mentor, OH 44060
Tel: (440) 953-8888
madicello@dicellolevitt.com

Counsel for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on August 18, 2022, I electronically filed the foregoing document with the Clerk of Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record or pro se parties either via transmission of Notices of Electronic Filing generated by CM/ECF or in some other authorized manner for those counsel or parties who are not authorized to receive electronically Notices of Electronic Filing.

/s/ Jeffrey P. Goodman